On Evaluating Delegated Digital Signing of Broadcasting Messages in 5G

Hui Gao*, Yiming Zhang†, Tao Wan‡, Jia Zhang*¶✉, Haixin Duan*‖

* Institute for Network Science and Cyberspace, Tsinghua University
† Department of Computer Science and Technology, Tsinghua University
‡ CableLabs & Carleton University
¶ Beijing National Research Center for Information Science and Technology (BNRist)
‖ Peng Cheng Laboratory
{gao-h19, zhangyim17}@mails.tsinghua.edu.cn, twan@scs.carleton.ca, zhangjia@cernet.edu.cn, duanhx@tsinghua.edu.cn

***Abstract*—In 5G networks, base stations, namely gNBs (5G NodeB, as per 3GPP nomenclature) periodically broadcast the system information messages including network identifiers to facilitate User Equipment (UE) to connect to the network. As in prior generations, the system information messages in 5G are transmitted in clear text without any security protection. Therefore, an adversary could spoof a legitimate gNB to become a man-on-the-side (MOTS) or man-in-the-middle (MITM) attacker. This vulnerability is being studied by 3GPP and a number of solutions have been proposed in the Technical Report (TR 33.809), including a promising solution namely Digital Signing Network Function (DSnF).**

In this paper, we provided an evaluation of DSnF, including the practicality of its assumption, feasibility of its certificate transmission within the system information message, and quantitative analysis of its performance. Our evaluation results show that DSnF is practical in general. Initial results from this paper have been provided to 3GPP and incorporated into TR 33.809.

***Index Terms*—Cellular Network, 5G, Broadcast, Fake Base-Stations**

I. Introduction

In cellular networks, base stations periodically broadcast frame synchronization signals and system information messages including the Master Information Block (MIB) and System Information Blocks (SIBs) to allow UE to discover and connect to the network. For example, a 5G gNB broadcasts the MIB every 80ms and SIB1 every 160ms. A UE scans supported frequencies for frame synchronization signals and system information and selects a gNB based on its signal strength and network preference. Once a gNB is selected, the UE can proceed to attach to the network by performing authentication and key agreement procedure with the network. If successful, the UE will be allocated a data bearer and connectivity to the Internet.

However, broadcasting messages in cellular networks from 2G to 5G are transmitted in clear text without any security protection, thus subject to spoofing or tampering attacks. For example, an adversary can exploit this vulnerability to carry out several serious attacks such as man-in-the-middle (MITM) [1], [2], [3], [4], downgrade attack [5], [6], [7] and alert messages spoofing [8]. The communication between the UE and the network could be eavesdropped, modified, or spoofed, resulting in serious security threats to the users. While mutual authentication and key agreement (AKA) between the UE and the network has been introduced since 3G, they are performed in the late stage after a UE acquires the clear text system information. Further, the existing AKA is based on a symmetric key shared between each UE and the network, which is not suitable for protecting broadcasting messages.

To further improve 5G security, 3GPP is studying potential solutions to provide authenticity of broadcasting system information. More specifically, several solutions based on digital signatures have been proposed in 3GPP TR 33.809 [9]. Among them, one solution namely Digital Signing Network Function (DSnF) is of our interest since it appears to be the most comprehensive proposal in 3GPP TR 33.809. In DSnF, system information including MIB and SIBs are digitally signed by the core network and broadcasted by gNBs. In this way, the private key used to sign the system information needs not be stored in gNBs, which may be located in some unsecured environment. Rather, the private key is stored in the core network, thus can be protected with the existing secure hardware used to protect other keying materials (e.g., AKA keys).

However, DSnF makes some assumptions which have not been validated in TR 33.809. Further, the performance analysis of DSnF is also anecdotal. In this paper, we use a real world test-bed to evaluate the practicality of the assumptions made by DSnF. We also provide quantitative performance analysis of DSnF. Initial results of our work have been provided to 3GPP and incorporated into TR 33.809. We hope this paper will further help 3GPP in its standardization effort to secure the system information. To summarize, this paper makes the following contributions:

- We collected the broadcasting system information from real cellular networks to empirically verify the assumption made by the DSnF that the system information is relatively static, allowing for pre-signing.
- We implemented a certificate delivery procedure using software-defined radios (SDR) and open source protocol

✉ Corresponding author

978-1-7281-8104-2/21/$31.00 ©2021 IEEE

stack to confirm that a public key certificate can be timely acquired by a UE to verify digitally signed system information of limited size.
- We provided a quantitative analysis of DSnF for its computational overhead, network bandwidth overhead, and end-to-end network delay.

The rest of the paper is organized as follows. Section II provides the basic concepts of cellular architecture and cell selection procedure. Section III describes the workflow of DSnF scheme. Section IV includes a measurement study and evaluation analysis. Section V reviews the existed work, and Section VI summarizes this paper.

II. Background

A. Cellular Architecture

A cellular network (as shown in Figure 1) consists of User Equipment (UE), Radio Access Network (RAN), and Core Network (CN).

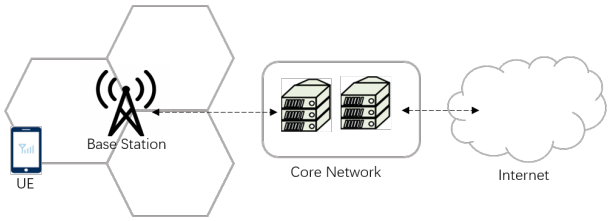

Fig. 1. Cellular network architecture

1) UE: A UE consists of a cellular device and a Universal Subscriber Identity Module (USIM) issued by a network operator. The USIM stores the identification information of a unique subscriber, e.g., the Subscription Permanent Identifier (SUPI) in 5G, and a secret key shared with the network operator. The secret key is used by the UE to perform the mutual Authentication and Key Agreement (AKA) procedure with the CN to acquire access to the cellular network.

2) RAN: A RAN consists of a number of base stations (e.g., gNBs in 5G) that allocate radio resources for the UE to access the cellular network via radio interfaces. RANs are connected to the CN via an IP network, which is often referred to as the backhaul network.

3) CN: The core network in 5G consists of a number of network functions including the Access and Mobility Management Function (AMF), the Authentication Server Function (AUSF) and Unified Data Management function (UDM), among others. The AMF is the network function in the CN to interface with RAN in the control plane and is responsible for the registration management and mobility management, among other critical services for the UEs.

B. Cell Selection Procedure

Cell selection is the first procedure performed by an UE after it powers on. As Figure 2 shows, a base station periodically broadcasts the frame synchronization signals and System Information (SI) messages. The SIs consist of the Master Information Block (MIB) and a set of System Information Blocks (SIBs). The MIB contains the minimal set of information (e.g., System Frame Number (SFN)) required to acquire other SIs. The SIBs contain scheduling and cell access information, among others.

The UE scans the synchronization signals in the allowed frequency bands, and identifies the suitable cells. The UE then reads the MIB and SIB1 for each candidate cell to find a preferred network based on the configuration in USIM. After selecting and camping on a cell, the UE initiates a connection to the base station at the Radio Resource Control (RRC) layer and the core network at the Network Access Stratum (NAS) layer. Unlike LTE in which all the MIB and SIBs are broadcasted periodically, 5G introduces a new approach to transmit the SI messages, namely on-demand delivery [10]. In 5G, the MIB and SIB1 are defined as minimum SIs, which are broadcasted periodically. The remaining SIBs (SIB2 to SIB9) are defined as other SIs, which are transmitted on demand when needed by a UE (as shown by the process in the dashed line, Figure 2).

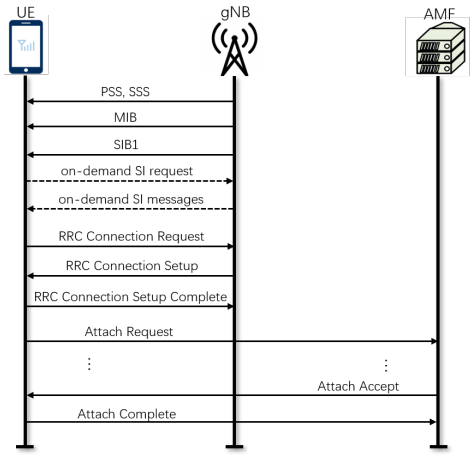

Fig. 2. Cell selection and initial connection procedure

C. Attacks from Cell Selection

Due to the fact that SIs are transmitted in clear text, the UE cell selection procedure can be manipulated to attack the UE, including man-in-the-middle (MITM) and man-on-the-side (MOTS) attacks.

MITM Attacks. An adversary can spoof a legitimate base station to become a malicious relay between an UE and the network. As a result, the adversary becomes a MITM and can eavesdrop and modify messages between the victim UE and the legitimate base station [1], [2], [3], [4].

MOTS Attacks. An adversary could lure the victim UE away from the legitimate base station to perform Denial of Service (DoS) attacks by rejecting service requests from the UE [11], [12], [13]. The adversary could also downgrade the UE to less secure GSM or 3G networks [5], [6], [7].

III. DSnF Scheme Workflow

In this section, we provide a brief overview of DSnF proposed in 3GPP TR 33.809 [9] and summarize its assumptions that we will validate in the real environment.

A. Overview of DSnF

As in prior generations, the system information messages in 5G are transmitted in clear text without any security protection. Thus, attacks exploiting this design flaw in prior generations of mobile networks are also effective in 5G. Although several defence schemes [14], [15], [16], [17] have been proposed to secure the system information messages in cellular networks, none of them has been accepted into 3GPP TR 33.809 to be considered as a candidate solution for 5G. One common issue of these schemes is that they require gNBs to perform expensive operations to digitally sign system information messages, incurring significant computational overhead in the gNBs. Moreover, they require the private keys for digital signing to be stored in gNBs, which may lack physical security and allow the private keys to be compromised.

DSnF uses digital signatures to provide the authenticity of broadcasting SIs. Instead of having SIs digitally signed by gNBs, SIs will be sent to 5G core network to be digitally signed. The purposes of delegating the signing of SIs to the core network are two-fold: to reduce the computational overhead in gNB and to protect the private key used for the signing. To mitigate replay attacks, additional attributes including Timestamp, Physical Cell ID (PCI) and downlink frequency are also digitally signed along with MIBs and SIBs. Figure 3 provides a high level call flow of DSnF.

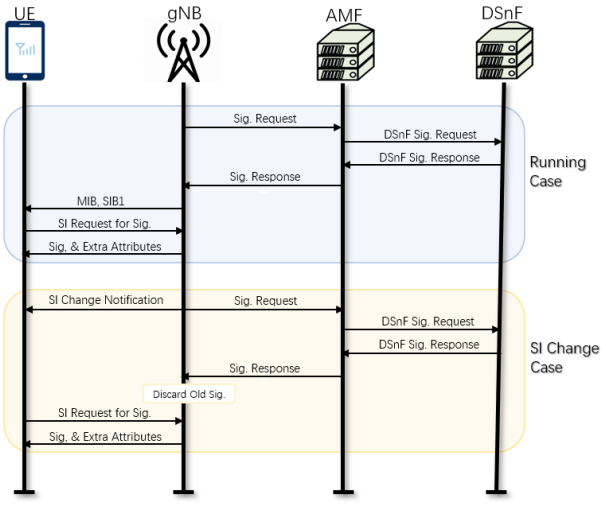

Fig. 3. Signature Request Procedure

B. Assumptions by DSnF

Since MIB and SIB1 are broadcasted in high frequent intervals of 80ms and 160ms respectively, it is unrealistic to expect that a gNB would send a digital signing request to the core network for each broadcast interval of MIB and SIB1. DSnF made the assumption that MIB and SIB1 are relatively static, thus can be pre-signed by the core network.

For example, a gNB can request digital signatures to be used for a certain period of time (e.g., an hour) during which the MIB and SIB1 are supposed to be static. More specifically, a gNB generates a digital signing request including a starting timestamp, time interval, ending timestamp, MIB and SIB1, and additional attributes to the DSnF. The DSnF will generate a set of digital signatures, one for each time interval, and send them back to gNB to be used until the ending time. The question is, *are MIB and SIB1 static in real network*?

Further, the public key certificate associated with the private key used to sign SIs need to be obtained by an UE in order to verify the signed SIs. Due to the limited size of MIB and SIB1, DSnF proposes to carry the public key certificate in a new SIB whose maximum size is 2,976 bits according to the 3GPP standard [18]. The second question is, *can a public key certificate (and potential certificate chain) be transmitted to the UE in time to allow the UE to verify the signed SIs to perform cell selection*?

We will validate these two questions in Section IV.

IV. Measurement and Evaluation

As discussed in [16], DSnF appears theoretically feasible in protecting broadcasting system information in 5G. However, it needs to be evaluated for its practicality and performance to allow 3GPP to make informed decision on whether or not it can be selected and standardized in 5G.

To fill this gap, we use real-world SDR based test beds to evaluate the two most important assumptions by DSnF: 1) whether system information is relatively static allowing delegated and batch signing, and 2) whether the public key certificate used to verify digitally signed system information can be acquired by UE in a timely manner. We also provide quantitative performance analysis of DSnF including its computational overhead, transmission overhead and end-to-end network delay.

A. Stability of MIB and SIB1

We conduct an empirical measurement study for the assumption of SI stability, by collecting the SI messages broadcast by real-world base stations and evaluate the content and frequency of changes. We first try to record SI messages captured by commercial UEs (Google Pixel 2) and to decode packets using QCsuper [19]. However, the frequency of obtained new SIs is too low (around 10min for a new scan, potentially limited by the base station connection and power saving policies of commercial handsets). We then establish the measurement using Software Defined Radio (SDR) equipment and open-source UE implementation. Specifically, we modify the attaching process of srsUE [20] to support a continuous capture of base station broadcast messages (around 3s interval for a new scan) and use Wireshark [21] as decoding tools. We separately collect MIBs and SIBs of a large mobile operator in 2 different provinces in China. The collection is conducted in the morning (9:00-10:00), afternoon (15:00-16:00) and evening (22:00-23:00) of each day, lasting for a whole week. We also test different SDR devices, including USRP B210 [22]

TABLE I
MIB AND SIB MEASUREMENTS

MIB Fields					
dl-Bandwidth	phich-Duration	phich-Resource	systemFrameNumber	schedulingInfo-SIB1-BR-r13	systemInfo-Unchanged-BR-r15
spare					
SIB1 Fields					
trackingAreaCode	cellIdentity	cellBarred	intraFreqReselection	intraFreq-Reselection	csg-Indication
q-RxLevMin	p-Max	freqBandIndicator	subframeAssignment	special-SubframePatterns	si-WindowLength
systemInfoValueTag	si-Periodicity	SIB-Type			

and USRP X310 [23], to avoid the impact of types of different SDRs.

The data sets show all information elements (in Table I) in MIB and SIB1 stay static in practice, except the system frame number (SFN), which increments by 1 each frame. According to the measurement results, signatures aggregation, namely pre-signing in batches is feasible for DSnF scheme.

B. Public Key Certificate Transmission

We next verify if a public key certificate can be obtained by an UE on demand using a new SIB as proposed by DSnF. We first describe the test bed on which we implemented the certificate transmission mechanism in DSnF.

Testbed Setup: Given that currently there is no mature open source 5G implementation available to us, we performed the experiments on a modified 4G test bed based on srsLTE [20]. Since the system information broadcasting procedure in 5G is similar to the basic broadcasting infrastructure in 4G [18], [24], we believe that the results from our experiments using 4G test bed are credible. Note other papers [14], [16] also used the 4G test bed to implement security proposed for 5G.

Specifically, we separately connected two USRP B210 [22] SDR boards to two Ubuntu 18.04 machines with Inter i7 Cores. One of them runs as the base station and the core network, the other as the user equipment. The software we implemented is srsLTE [20].

We consider three methods that are supported by 5G standards for delivering messages to UEs, including periodic broadcast, on-demand broadcast, and on-demand broadcast with Listen Before Request (LBR) model. The details and parameter notations (see Table II) are described below.

Periodic Broadcast (PB): Periodic broadcast is used for basic SI messages in 5G. Considering the DSnF scheme uses an opt-in mode, periodic broadcast is not an economical approach to deliver public key certificates and is not used by DSnF. Thus, we did not implement this method for certificate delivery. To facilitate quantitative performance analysis, here we model the signaling overhead and the UE power consumption. Considering the signaling overhead (the bytes transmitted) Ω_s, in periodic broadcasting case, only the broadcast SIBs are transmitted and the resources used by each beam are the same. We simply denote the size of SIBs as the same value B_{SI} and the amount of SI kinds as K. Then the signaling overhead could be the product of them. For the UE power consumption Ω_p, as UE only receives SIB in the SI window, we could get its equation:

$$\Omega_s = B_{SI} \times \nu \times K, \Omega_p = e_{SI} \times \lambda. \tag{1}$$

On-demand broadcast (OB): On-demand broadcast is an economical approach introduced in 5G for gNBs to transmit SI messages. When the UE sends SI requests, the gNB replies with corresponding SI messages. This is used by DSnF to deliver the public key certificate to UE.

We implemented on-demand broadcast in srsLTE. We first modified srsLTE stack [20] to allow an UE to send SI requests by adding an additional bit of RACH preamble (MSG1). This allows a base station to check whether or not a new SI needs to be transmitted. Since 4G does not support on demand SIB transmission, we then modified the open-source srsLTE stack to add a new SIB to verify the on-demand delivery mechanism. Our implementation confirms that a SIB can be transmitted to UE on demand. However, the new SIB is still subject to the size limit of 2,976 bits [18], thus cannot carry a standard X.509v3 certificate chain.

In the on-demand broadcast case, three messages are delivered during SIB transmitting process. The first one is the RACH preamble, for which the overhead is fixed as $B_1 \times \nu \times K$. Second, the MSG2 of random access procedure is transmitted by the base station beam, thus the signaling overhead is related to the number of used preambles $M_{p,L'}$. Third, as the base station will broadcast the SIB once it receives the request, the probability that receiving the request is equal to that broadcasting the SIB, denoted as γ and could be assumed to conform to Poisson Distribution. The probability that a base station receives a request to broadcast a SIB could be assumed to conform to Poisson Distribution:

$$\gamma = 1 - e^{-\frac{\lambda T_b}{\nu}}. \tag{2}$$

So we have the following quantifications:

$$\Omega_s = (B_1 + B_2 \times E[M_{p,L'}] + B_{SI} \times \gamma) \times \nu \times K, \tag{3}$$

$$\Omega_p = (e_1 + e_2 + e_{SI}) \times \lambda. \tag{4}$$

On-demand broadcast with LBR (OB-L): On-demand broadcast with LBR requires a UE to monitor the channel for a SIB before sending the request. This can reduce the signaling overhead on gNB, especially in congested situations.

We denote the probability for the base station to receive more than one successful on-demond SIB requests as β, which also follows a Poisson Distribution, i.e., $\beta = 1 - e^{-\frac{\lambda T_b}{\nu}}$. Let the probability that the base station broadcasts one SIB with LBR in the period be γ_L^t, then the probability of broadcast could be solved by the following Markov Chain:

$$\begin{bmatrix} \gamma_L^{t+1} \\ 1 - \gamma_L^{t+1} \end{bmatrix} = \begin{bmatrix} 0 & \beta \\ 1 & 1 - \beta \end{bmatrix} \begin{bmatrix} \gamma_L^t \\ 1 - \gamma_L^t \end{bmatrix}. \tag{5}$$

TABLE II
THE NOTATIONS USED IN THE ANALYSIS

Notation	Description
Ω_s	The signaling overhead that the base station consumes in a period
Ω_p	The power that UEs consume for receiving SIB in a period
B_{SI}	The size of SIB
B_1, B_2	The size of MSG1/MSG2
ν	The number of base station beams
K	The number of other SI's kinds
e_{SI}	The energy consumed by the UE when the UE receives the SIB
e_1, e_2	The energy consumed by the UE when the UE transmit or receive the MSG1/MSG2
λ	The arrival rate of SIB under one base staion
γ	The probability that one base station beam broadcasts the SIB
T_b	The period length of the SI window.
t	The variable that represents a period of SI window.
$M_{p,L}, M_{p,L'}$	The number of preambles used in one beam area with / without LBR
β	The probability that one base station receives more than one SIB request
N_{gNB}	The number of served gNB
T_{valid}	The period of validity of signatures
N_{sig}	the number of signatures in each signing request

By solving the equation (5) in steady state, we get:

$$\gamma_L = \frac{\beta}{1+\beta} = \frac{1 - e^{-\frac{\lambda T_b}{\nu}}}{2 - e^{-\frac{\lambda T_b}{\nu}}}. \quad (6)$$

Similarly, overhead and consumption could be calculated as:

$$\Omega_s = (B_1 + B_2 \times E[M_{p,L}] + B_{SI} \times \gamma_L) \times \nu \times K, \quad (7)$$

$$\Omega_p = e_{SI} \times \lambda + (1 - \gamma_L) \times (e_1 + e_2 + e_{SI}) \times \lambda. \quad (8)$$

RRC Unicast Method: In addition to the on-demand broadcast method used by DSnF, we also propose a new approach to transmit protected messages using RRC connection without the initial security activation, i.e., without the initial configuration of AS integrity protection (SRBs) and AS ciphering (SRBs, DRBs). Figure 4 shows the details. This method is inspired by [25] which uses RRC connection to transmit on-demand system information.

This unicast approach can bypass the size limitation of SIB messages and deliver standard X.509v3 certificates or certificate chains, allowing the support of any trust model as proposed by DSnF in TR 33.809. For backward compatibility, this mechanism could be set to an opt-in mode, i.e., the certificate will be transmitted only if the UE supports this scheme and requests for it.

We implemented this method in srsLTE based on the data structure in RRC layer but without using the codes for establishing RRC layer security context. Our experiment confirmed that this method is practical. Although incurring additional communication overhead, it can be used to deliver X.509v3 certificate and chains, thus allowing to use any trust model proposed in DSnF.

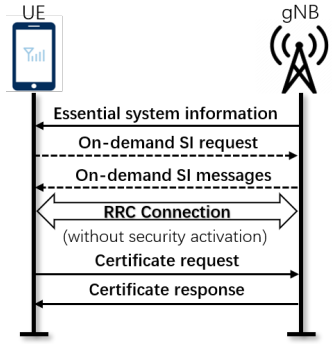

Fig. 4. Certificate transmission using RRC Connection without the initial security activation

TABLE III
BYTES OVERHEAD OF RELATED ATTRIBUTES

Field	Size (bytes)
MIB (without extension)	3
SIB (max size)	372
Timestamp	4
Downlink Frequency	4
Physical Cell ID	2
DSnF Signature	64

C. Quantitative Performance Analysis

In 3GPP TR 33.809, DSnF is evaluated for its performance only using some sample network configurations. To allow the evaluation to apply to any network configuration, we fill the gap by providing a quantitative analysis of its performance, including computational overhead, network bandwidth overhead, and end-to-end network delay.

Since 3GPP standard [26] recommends the RSA and ECDSA algorithm for public key certificates, we choose ECDSA-256 for the evaluation due to its smaller key length and certificate size. Table III shows the byte overhead of MIB, SIB1, and additional attributes. Those values are based on the prior analysis work [25], where B_{SI} = 70 bytes, B_1 = 64 bits, B_2 = 56 bits, ν = 2, T_b = 0.1.

End-to-end delay: The end-to-end delay is defined as the time between when SIB1 messages are generated and when the UE verifies signatures in the new SIB for DSnF scheme. Table IV shows the end-to-end overhead of the baseline (not modified for signatures), the ECSDA-224 Periodic Broadcast* in the previous work [14] and DSnF scheme, on-demand broadcast and RRC connection without the initial security activation. According to the results, DSnF scheme (on-demand broadcast and RRC connection) induces additional transmission overhead against baseline and ECSDA-224 Periodic Broadcast*. Because the UE needs not to acquire SIB messages frequently and the pre-signing in batches of DSnF saves the generation overhead, the end-to-end overhead of DSnF scheme is acceptable. In addition, there is not a sharp distinction between the overhead of RRC connection approach and that of on-demand approach.

Computational overhead: Table V shows the computational overhead based on the results from a PC with Intel i7 core CPU. The verifying overhead is depending on the

TABLE IV
END-TO-END DELAY

	Gener. (ms)	Trans. (ms)	Verify (ms)
Baseline	0	171	0
ECDSA-224 Periodic Broadcast*	1.21	210	6.81
On-Demand Broadcast	0	236	6.67
RRC Connection	0	243	6.92

TABLE V
COMPUTATIONAL OVERHEAD

	Generate		Verify	
	Avg.(ms)	SD(ms)	Avg.(ms)	SD(ms)
DSnF's sig.	1.003	0.016	3.394	0.494
Core Network's sig.	1.002	0.01	3.282	0.453

CPU platform, and this evaluation provides a lower bound for the UE's computational overhead. The core network signature is computed by the core network offline, and could be sent to gNB before it boots up. Since the UE typically verifies the signature only once when acquiring the SIB message, the impact of verifying the signature is much smaller.

Signaling overhead of BS and UE: We evaluate the signaling overhead of periodic broadcast, on-demand broadcast and on-demand broadcast with LBR. As Figure 5 shows, when the arrival rate of SIB requests is low, the on-demand mechanism is more effective than periodic broadcasting. After the arrival rate exceeds the cross point of PB and OB curves (i.e., 33 arrivals/second), the on-demand mechanism incurs more transmission overhead than the periodic broadcasting. However, the on-demand with LBR mechanism can further reduce the transmission overhead and always performs better than the periodic broadcasting. Figure 6 shows both OB and OB-L introduce extra energy consumption overhead to the UE. According to [18], UE can cache acquired SIs for up to 3 hours. Since the initial connection process does not happen often for the UE, the extra overhead introduced by OB and OB-L to the UE is considered acceptable.

Communication overhead between DSnF and BS: Since the AMF needs to interact with a number of base stations, the communication overhead is directly proportional to the number of served base stations (N_{BS}) and the number of signatures (N_{sig}) in each signing request, and is inversely proportional to the validity period of a signature ($T_{interval}$). The following formula provides an estimation of the communication overhead:

$$\Omega_{req} = \frac{B_{req} \times N_{BS}}{T_{interval} \times N_{sign}}, \Omega_{resp} = \frac{B_{resp} \times N_{BS}}{T_{interval} \times N_{sign}}. \quad (9)$$

According to the values in Table V, Figure 7 shows the overhead of signing requests under different N_{sig}. We could conclude that the increase of N_{sig}, namely pre-signing signatures in batches, would significantly reduce the communication overhead. We consider a set of sample parameters, where N_{BS} = 100, $T_{interval}$ = 10.24 s, B_{req} = 372 B, B_{resp} = 64 B. The bandwidth overhead of request is around 314M per day. If each request asks for 60 signatures (for next 10 minutes), the bandwidth would be reduced to 5.2 M per day.

D. Summary of evaluation

The measurement study shows the fields in MIB and SIB1 stay relatively static in practice, and pre-signing in batches is feasible for DSnF scheme. The implementation on real testbeds reveals a public key certificate can be timely acquired by a UE to verify digitally signed SI. The quantitative analysis shows DSnF scheme could be deployed in 5G without leading to substantial overhead. In large networks, considering the increase of the SI requests rate and the numbers of gNBs served by a DSnF module, using on-demand mechanism with LBR and pre-signing signatures in batches could significantly reduce the signaling overhead and communication overhead. Besides, utilizing standard certificates while circumventing the length limit of SIB messages by RRC connection method is also a feasible option for DSnF.

V. RELATED WORK

Although several schemes have been proposed to secure the bootstrapping procedures in cellular networks, none of them has been accepted into 3GPP TR 33.809 to be considered as a candidate solution for 5G. Hussain et al. [14] proposed a PKI-based authentication mechanism for broadcasting messages. Their scheme has certain security properties but is based on an asymmetric crypto algorithm BGLS not approved by 3GPP. Thus, this scheme is unlikely to be accepted by 3GPP. Another defense scheme [15] could assist in securing the location update procedure, but does not apply to cell authenticity verification in the initial registration procedure. Singla et al. [16] proposed an Identity Based Signature (IBS) scheme. Although this scheme performs well with low computational overhead, it is not considered suitable for the cellular bootstrapping scenario due to the need to first establish a secure channel to transmit the private key, as discussed in [17].

Besides, various security schemes have been proposed to detect fake base stations (FBSs). Zhuang et al. [27] identify FBS devices based on the minor difference in the emitted signals caused by hardware imperfections. Arslan et al. [28] propose a promising carrier frequency offset (CFO) based RF fingerprinting scheme, which could detect low, medium and high performing FBS. Huang et al. [29] include the location information of UE and base station and detect FBSs using the average received synchronization signal strength (ARSSS) from base station according the path loss, shadowing effect and small-scale fading. Although these solutions could be effective in detecting FBS attacks, enhancing the security of bootstrapping process, as the capability of DSnF, could mitigate this issue in a more fundamental way.

VI. CONCLUSION

This work evaluates DSnF, a 5G bootstrapping security solution. By collecting and analyzing real-world broadcast system information messages in cellular networks, and implementing the certificate delivery procedure through SDRs and modified open source protocol stacks, we provide the verification of two important assumptions of DSnF. We also give a quantitative analysis of its performance. Our results prove that DSnF is

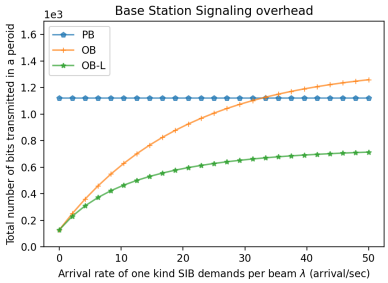

Fig. 5. The signaling overhead of above 3 options (periodic broadcast (PB), on-demand broadcast (OB) and on-demand broadcast with LBR (OB-L)) changes over the arrival rate of UE's demands.

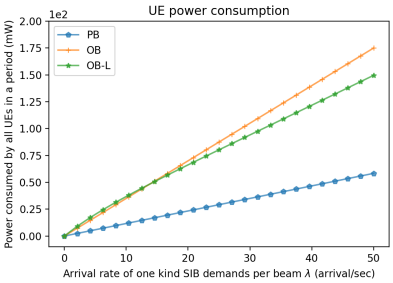

Fig. 6. The UE power consumption of above 3 options (periodic broadcast (PB), on-demand broadcast (OB) and on-demand broadcast with LBR (OB-L)) with arrival rate of SI demands.

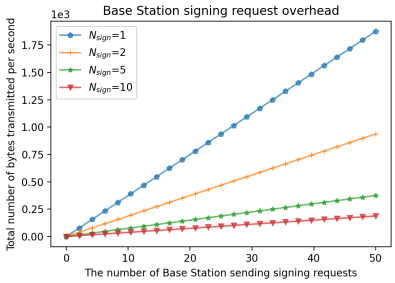

Fig. 7. BS Signing requests overhead

generally practicable. The initial version of our work has been provided to 3GPP and incorporated into TR 33.809.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (U1836213, U1636204) and the BNRist Network and Software Security Research Program (Grant No. BNR2019TD01004).

REFERENCES

[1] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking lte on layer two," *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121–1136, 2019.

[2] ——, "Imp4gt: Impersonation attacks in 4g networks," in *ISOC Network and Distributed System Security Symposium (NDSS)*, 2020.

[3] K. Kohls, D. Rupprecht, T. Holz, and C. Pöpper, "Lost traffic encryption: fingerprinting lte/4g traffic on layer two," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 249–260.

[4] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "Lteinspector: A systematic approach for adversarial testing of 4g lte," 2018.

[5] L. Huang, "Forcing targeted lte cellphone into unsafe network," in *HITB AMS Security Conference*, 2016.

[6] C. Yu, S. Chen, and Z. Cai, "Lte phone number catcher: A practical attack against mobile privacy," *Security and Communication Networks*, vol. 2019, 2019.

[7] S. F. Mjølsnes and R. F. Olimid, "Easy 4g/lte imsi catchers for non-programmers," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 2017, pp. 235–246.

[8] G. Lee, J. Lee, J. Lee, Y. Im, M. Hollingsworth, E. Wustrow, D. Grunwald, and S. Ha, "This is your president speaking: spoofing alerts in 4g lte networks," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 2019, pp. 404–416.

[9] 3GPP, "Study on 5G Security Enhancement against False Base Stations (FBS)," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 33.809, 12 2020, version 0.12.1.

[10] ——, "NR; NR and NG-RAN Overall Description; Stage 2," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.300, 07 2020, version 16.2.0.

[11] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," 2016.

[12] Y. Chuan and S. Chen, "On effects of mobility management signalling based dos attacks against lte terminals," in *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2019, pp. 1–8.

[13] R. P. Jover, "Lte security, protocol exploits and location tracking experimentation with low-cost software radio," *arXiv preprint arXiv:1607.05171*, 2016.

[14] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: the root of all evil," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 1–11.

[15] Apple, "Verification of authenticity of the cell," 3rd Generation Partnership Project (3GPP), Technical Document (TDoc) S3-200991, 05 2020.

[16] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "Look before you leap: Secure connection bootstrapping for 5g networks to defend against fake base-stations," in *Proceedings of the 2021 Asia Conference on Computer and Communications Security*, 2021.

[17] H. Phaneendra *et al.*, "Identity-based cryptography and comparison with traditional public key encryption: A survey," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 4, pp. 5521–5525, 2014.

[18] 3GPP, "NR; Radio Resource Control (RRC) protocol specification; Protocol specification," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.331, 07 2020, version 16.1.0.

[19] "QCsuper." [Online]. Available: https://github.com/P1sec/QCSuper

[20] "Open Source SDR LTE Software Suite (srsLTE)." [Online]. Available: https://github.com/srsLTE/srsLTE

[21] "Wireshark." [Online]. Available: https://www.wireshark.org/

[22] "Ettus Research USRP B210." [Online]. Available: https://www.ettus.com/product/details/UB210-KIT

[23] "Ettus Research USRP B210." [Online]. Available: https://www.ettus.com/all-products/x310-kit/

[24] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA);Radio Resource Control (RRC)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 36.331, 03 2020, version 16.0.0.

[25] W.-Y. Yang, K.-H. Lin, and H.-Y. Wei, "5g on-demand si acquisition framework and performance evaluation," *IEEE Access*, vol. 7, pp. 163 245–163 261, 2019.

[26] 3GPP, "Network Domain Security (NDS); Authentication Framework (AF)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.310, 07 2020, version 16.4.0.

[27] Z. Zhuang, X. Ji, T. Zhang, J. Zhang, W. Xu, Z. Li, and Y. Liu, "Fbsleuth: Fake base station forensics via radio frequency fingerprinting," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 261–272.

[28] A. Ali and G. Fischer, "The phase noise and clock synchronous carrier frequency offset based rf fingerprinting for the fake base station detection," in *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*. IEEE, 2019, pp. 1–6.

[29] K.-W. Huang and H.-M. Wang, "Identifying the fake base station: A location based approach," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1604–1607, 2018.